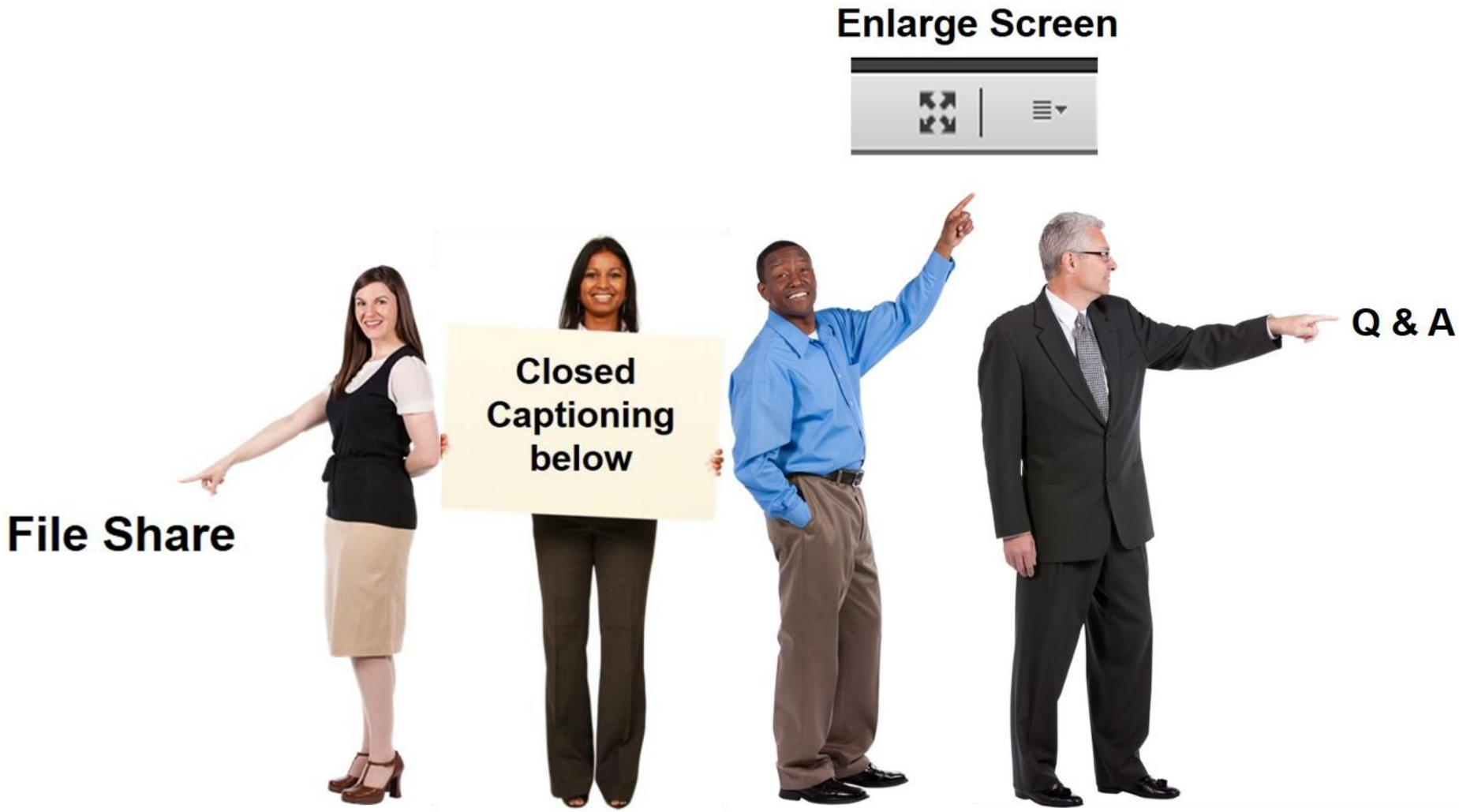
INDUSTRIAL SECURITY

POLICY CHANGES WEBINAR

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

ADOBE CONNECT



SPEAKERS

Jason Steinour

Industrial Security Curriculum Manager

Center for Development of Security Excellence

Allyson Renzella

Industrial Security Policy Analyst

OUSD(I&S)

Keith Minard

Senior Policy Advisor

Defense Counterintelligence and Security Agency

AGENDA

- NISPOM, 32 CFR Part 117
- Major Changes
- Tools
- Implementation Requirements
- Industrial Security Letters (ISLs)
- SEAD 3
- Controlled Unclassified Information (CUI)
- DCSA Processes
- Conclusion

NIPSOM OR 32 CFR PART 117?

- 32 Code of Federal Regulations (CFR) Part 117 was published on December 21, 2021

- 32 CFR Part 117 became effective on February 24, 2021
  - DOD Manual 5220.22 National Industrial Security Operating Manual (NISPOM) will soon be canceled

- Which is it now and how do we refer to it?
  - NISPOM is still “NISPOM”
  - It is also 32 CFR Part 117

MAJOR POLICY CHANGES

- Format Changes
  - Format and paragraph numbering are different

- Key Changes
  - Granting FCLs
  - SMO duties
  - TS accountability
  - IDS installation
  - Safeguarding
  - Classified Information Retention
  - Section 842 Public Law 115-232
  - Incorporation of SEAD 3 reporting requirements
  - Two types of limited FCLs

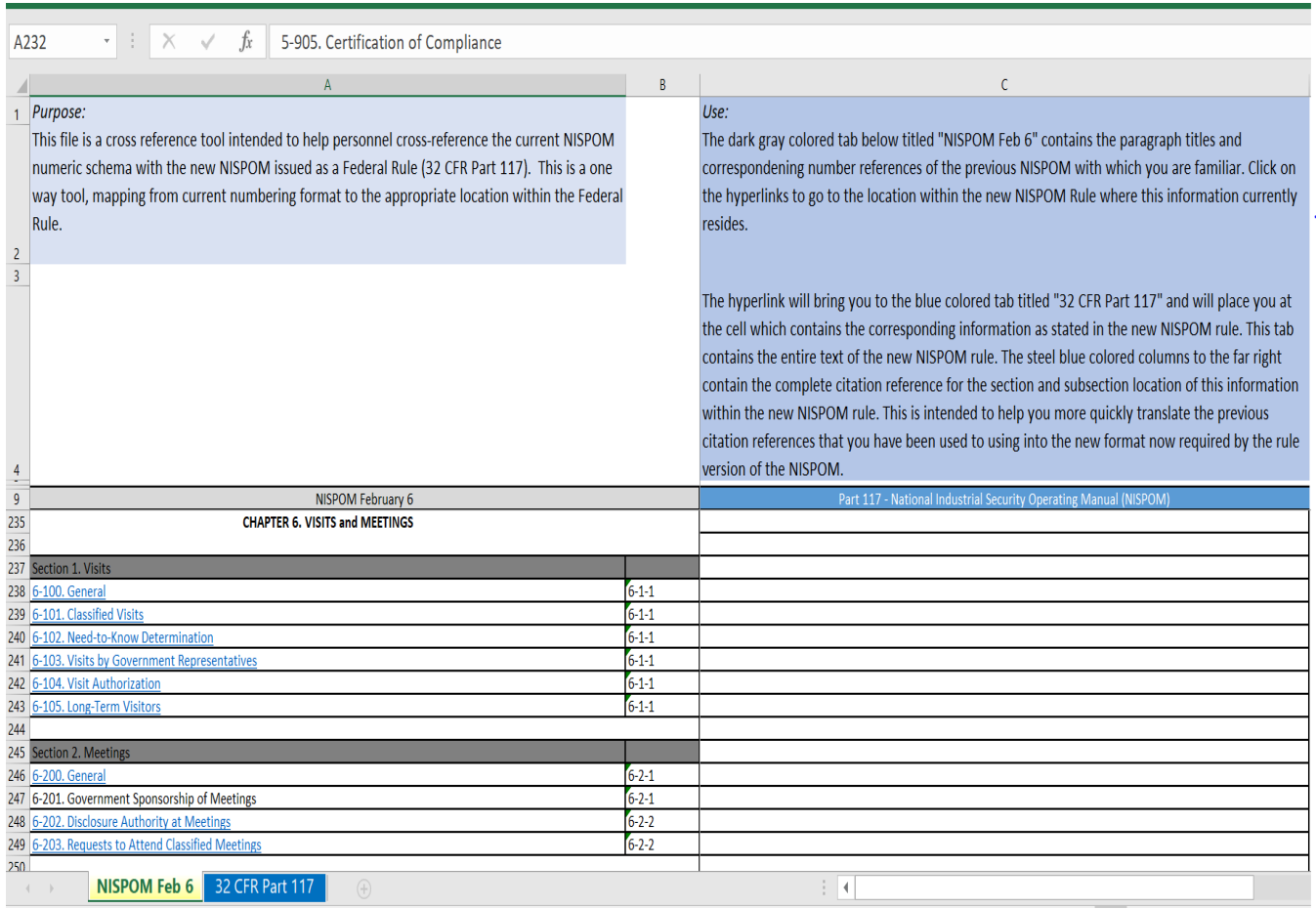
POLL QUESTION 1

- Are you familiar with the tools to assist with the NISPOM or 32 CFR Part 117 changes?

  - Yes
  - No
  - Not sure

TOOLS TO ASSIST WITH CHANGES

- List of major changes in the preamble of the Rule
- 32 CFR Part 117 NISPOM Rule Cross Reference Tool
  - Click on a NISPOM citation to be shown the CFR Rule
  - Located on the CDSE Website on the Industrial Security Homepage and in the FSO Toolkit

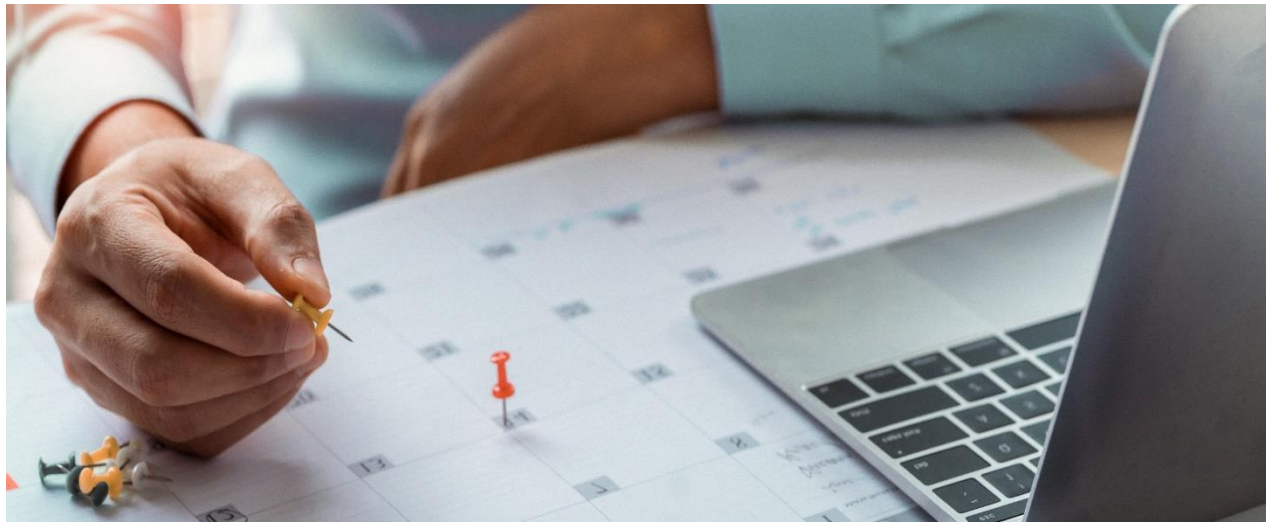


POLL QUESTION 2

- How long do contractors have until all requirements must be fully implemented?

  - 3 months
  - 6 months
  - 9 months
  - 12 months

IMPLEMENTATION REQUIREMENTS



- Implementation deadline: six months from effective date (August 2021)
  - Actual date will be noted in ISL
- Security programs must be in compliance by implementation deadline
  - Areas not in compliance will be cited as vulnerabilities

CITING REFERENCES

- Citing NISPOM references
  - Ex. 1-302.b. Suspicious Contacts → 32 CFR Part 117.8(C)(2).
- DCSA:
  - Updating tools, oversight guidance, and systems, including training and resources located on the DCSA Website
- Industry:
  - Don’t wait, start now to update your tools and products to support your program
  - Use available tools such as the cross reference tool on the DCSA website

INDUSTRIAL SECURITY LETTERS (ISLs)

- DCSA staffed ISL coordination with the NISPPAC for 32 CFR Part 117 and SEAD 3 Requirements

- Existing ISLs have been reviewed and a determination has been made for rescinding or reissuance

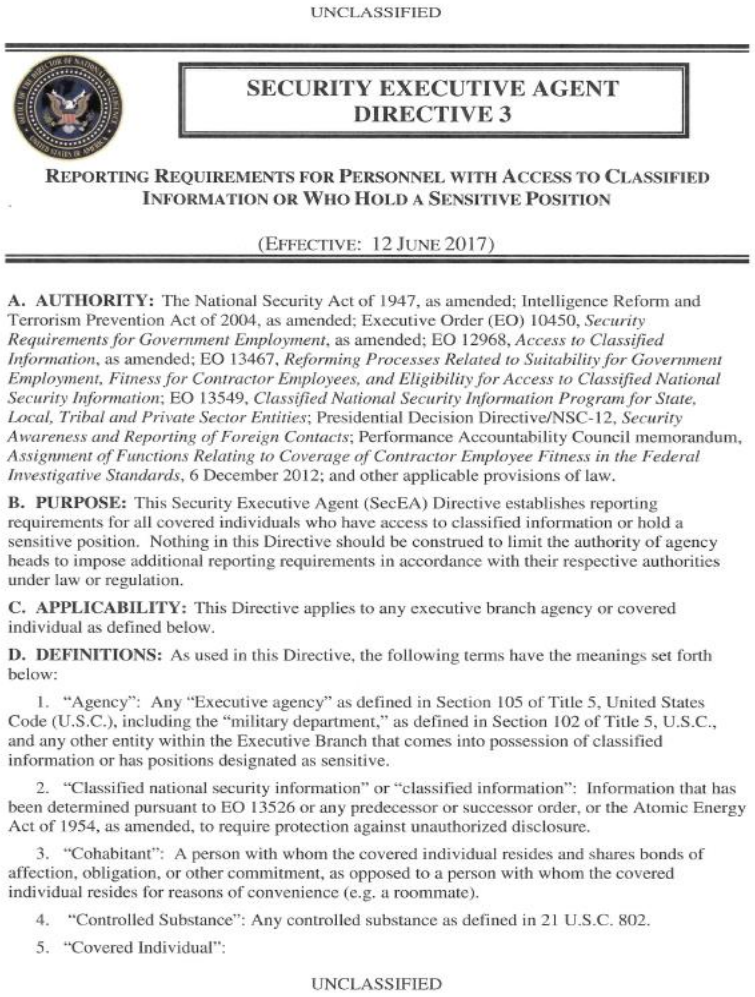
POLL QUESTION 3

- Are you familiar with the Security Executive Agent Directive (SEAD) 3?

  - Yes
  - No
  - Not sure

Security Executive Agent Directive (SEAD) 3

- SEAD 3 and other SEADs are included in the Rule
- ISL will provide additional CSA guidance
- ISL Implementation requires coordination
  - DCSA
  - CTP Directorate
  - VROC
  - Program Executive Office



UNCLASSIFIED

SECURITY EXECUTIVE AGENT DIRECTIVE 3

REPORTING REQUIREMENTS FOR PERSONNEL WITH ACCESS TO CLASSIFIED INFORMATION OR WHO HOLD A SENSITIVE POSITION

(EFFECTIVE: 12 JUNE 2017)

A. AUTHORITY: The National Security Act of 1947, as amended; Intelligence Reform and Terrorism Prevention Act of 2004, as amended; Executive Order (EO) 10450, *Security Requirements for Government Employment*, as amended; EO 12968, *Access to Classified Information*, as amended; EO 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*; EO 13549, *Classified National Security Information Program for State, Local, Tribal and Private Sector Entities*; Presidential Decision Directive/NSC-12, *Security Awareness and Reporting of Foreign Contacts*; Performance Accountability Council memorandum, *Assignment of Functions Relating to Coverage of Contractor Employee Fitness in the Federal Investigative Standards*, 6 December 2012; and other applicable provisions of law.

B. PURPOSE: This Security Executive Agent (SecEA) Directive establishes reporting requirements for all covered individuals who have access to classified information or hold a sensitive position. Nothing in this Directive should be construed to limit the authority of agency heads to impose additional reporting requirements in accordance with their respective authorities under law or regulation.

C. APPLICABILITY: This Directive applies to any executive branch agency or covered individual as defined below.

D. DEFINITIONS: As used in this Directive, the following terms have the meanings set forth below:

1. "Agency": Any "Executive agency" as defined in Section 105 of Title 5, United States Code (U.S.C.), including the "military department," as defined in Section 102 of Title 5, U.S.C., and any other entity within the Executive Branch that comes into possession of classified information or has positions designated as sensitive.

2. "Classified national security information" or "classified information": Information that has been determined pursuant to EO 13526 or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure.

3. "Cohabitant": A person with whom the covered individual resides and shares bonds of affection, obligation, or other commitment, as opposed to a person with whom the covered individual resides for reasons of convenience (e.g. a roommate).

4. "Controlled Substance": Any controlled substance as defined in 21 U.S.C. 802.

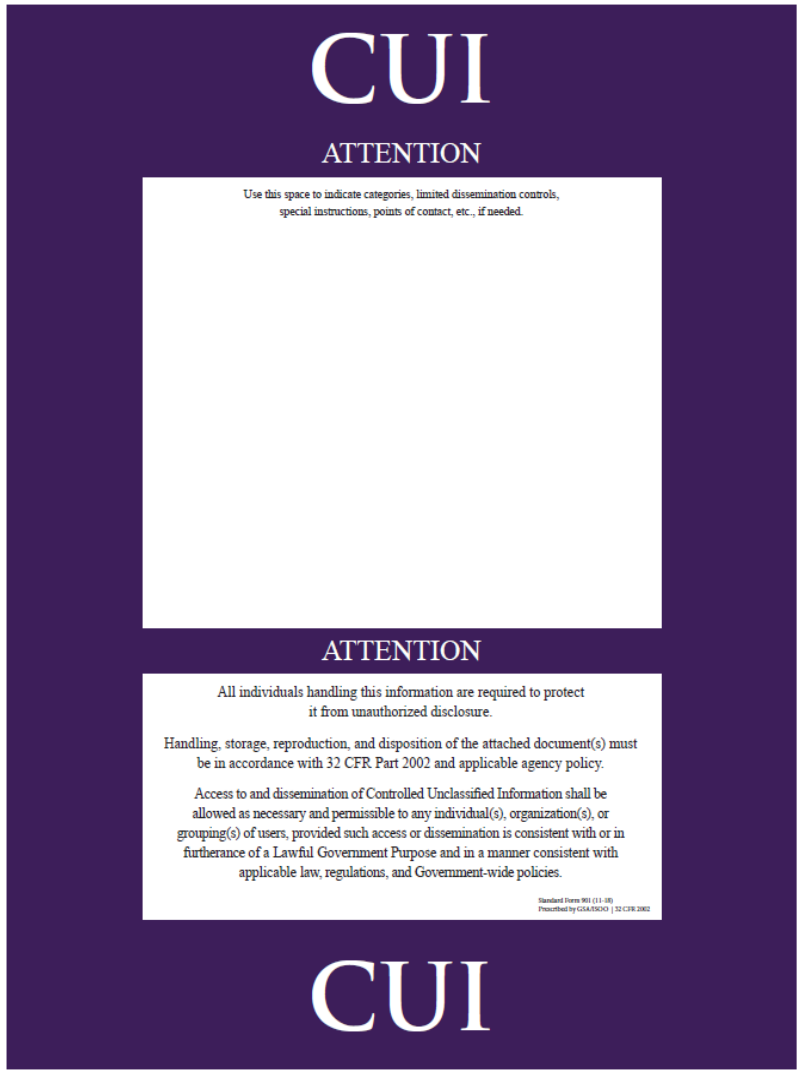
5. "Covered Individual":

UNCLASSIFIED

https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-Reporting-U.pdf

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

- 32 CFR Part 117
  - References CUI
    - Safeguarding
    - Training
    - Marking
  - CUI is out of the scope of the NISPOM, but:
    - Classified contracts may have CUI provisions



DCSA PROCESSES

- Security Vulnerability Assessments (SVAs)
  - Alignment with 32 CFR Part 117
  - Similar process to current state for assessing security programs
- ISR Training
  - Field training – train the trainer
  - Common communication platform
  - Training and informational sessions
- Security Rating System
  - Evaluate processes

KEY TENANTS OF IMPLEMENTATION STRATEGY

- Manage Cultural Change
- Collaboration and Partnership
- Communicate - Frequently and Clearly
- Focus on Major Changes
- Address Industry Input
- Deliver Capabilities
- Revise Oversight
- Train the Workforce
- Address Challenges

CONCLUSION

- 32 CFR Part 117, NISPOM
- Major changes: formatting and content changes
- Tools: preamble and “32 CFR Part 117 NISPOM Rule Cross Reference Tool”
- Implementation requirements: six months from the effective date
- ISLs forthcoming for 32 CFR Part 117 and SEAD 3
- Controlled Unclassified Information (CUI)
- DCSA processes: SVAs, IS Rep training, Security Rating evaluation
- Key tenants of DCSA’s implementation strategy

Questions?